論文の内容の要旨

論文題目　Provably-Secure Remote User Authentication Without Special Devices
特別な装置を持たない利用者の遠隔認証とその証明可能安全性に関する研究

氏　名　古原　和邦

1990年代に商用利用の始まったインターネットは、WWW (World Wide Web) の出現、i-mode, WAP (Wireless Application Protocol) などを用いた携帯電話からの利用、WLAN (Wireless LAN) やデータ通信カードを用いたPDA (Personal Digital Assistance) やノートＰＣなどからの利用、xDSL (Digital Subscriber Line) などの広帯域接続の低価格化などにも助けられ、普及の一途をたどり続けている。また、インターネット上で提供されるサービスも増加し、その範囲は、コンテンツのダウンロードや社内LANへの接続からモバイルバンキングやモバイルトレーディングなどまで多岐にわたる。

インターネット上のサービスはインターネットに接続できさえすれば原則どこからでも利用できるという利点を持つが、利用者認証はその分厳密かつ安全に行う必要がある。例えば、インターネットカフェやキオスク端末などの公共の場所からインターネットに接続する際には、パスワードののぞき見などに注意する必要がある。また、自分の端末を外出中で利用する際には、端末の置き忘れや盗難などにも注意する必要がある。さらに、ネットワーク上では盗聴やサーバへの成りすましが行われている可能性もあり、それら全てに的確に対処する必要がある。

本研究では、以下のような状況において遠隔地にいる利用者を安全かつ安価に認証する方法、およびその安全性に関する研究を行う。まず、利用者の利用する端末はどこにでもある通常の端末を仮定する。つまり、ディスプレイとキーボードのみをユーザインターフェースとして備えており、身体的特徴を読み取る特殊な装置や耐タンパー装置などは備えていないものとする。この種の端末は特別なものではないため、どこにいても安価に調達できるという利点がある。次に、攻撃者としては、現実世界の攻撃者とネットワーク上の攻撃者を仮定する。現実世界での攻撃者は、認証の際に利用者

に表示される画面と利用者の打ち込んだ情報を全てをのぞき見ることができるものとし、また、利用者が自分専用の端末（PDA、携帯電話、ノートＰＣなど）を持っている場合には、それらも入手可能であるとする。ネットワーク上の攻撃者は、ネットワークに流れる全データの盗聴、および偽のサーバを立ち上げそこに利用者を導き認証を行わせることができるものとする。

上記のような状況においても、安全かつ安価に遠隔地の利用者を認証することが本研究の目的であり、これに関して得られた結果を以下のような構成で記述する。まず、第１章では本学位論文で想定する環境や攻撃に関する説明を行う。第２章では、現実世界の攻撃者への対処方法として質問応答個人認証方式をとりあげ、そののぞき見に対する耐性の厳密な評価をおこなう。また、質問の出し方を制御することにより耐性を向上させる方法の提案を行う。現実的な値を用いた場合、質問応答個人認証方式は１回程度ののぞき見にしか対処できないが、質問の出し方を制御することで、数回までののぞき見に対処できることを示す。第３章では、のぞき見に対する耐性を飛躍的に向上させる方法を提案する。具体的には、視覚復号型秘密分散方式を用いて可視空間を制限する方法を提案し、その可視空間特性を解析する。結果、特定の場所にいる利用者のみに情報を伝えることが可能であることを示す。このことは、質問応答個人認証方式と組み合わせることにより現実世界で行われるのぞき見に対処できることを意味する。この方式では利用者にスライドを持たせることになるが、これらのスライドが攻撃者に盗まれたとしても、攻撃者は利用者の秘密に関して何の情報も得ることはできないという利点を持つ。

第４章では、ネットワーク上で行われる攻撃を公開鍵暗号を用いて対処することを考える。すべての公開鍵暗号がネットワーク上で行われる攻撃に対して理想的な安全性を持っているとは限らないため、この章では理想的な公開鍵暗号を構成する方法に関する研究を行う。具体的には、関数の形によって（原始的な）公開鍵暗号を決定的関数、部分落し戸関数、完全落し戸関数に分類して、各関数がある条件を満たす場合にそれらを理想的な公開鍵暗号に変換する方法を提案する。また、線形符号の復号問題に基づく原始的な公開鍵暗号方式の安全性を評価し、それらがその条件を満たすことを示す。これらの結果より、ネットワーク上の攻撃は理想的な公開鍵暗号を用いることで対処可能であり、また、そのような暗号方式を構成することも可能であることを示す。公開鍵暗号を用いる対処方法は、しかしながら、利用者にサーバの公開鍵（もしくはその拇印）を持たせる必要がある。そこで第５章では、利用者が公開鍵を持たずにネットワーク上の攻撃に対処できる方式としてパスワード認証された鍵交換方式をとりあげ、その改良を行う。我々は、計算量および通信量の少ない方式を提案し、その方式の安全性が決定 Diffie-Hellman 問題に帰着できることを特殊な仮定を用いることなく示す。

第６章では全体の総括を行う。現実世界での攻撃は質問応用個人認証と可視空間を制限する視覚復号型個人認証方式を組み合わせることにより対処可能であり、ネットワーク上での攻撃は理想的な公開鍵暗号方式もしくはパスワード認証された鍵交換方式を用いることにより対処可能である。